Statement of the Honorable Greg Walden
Subcommittee on Communications and Technology
Hearing on "Cybersecurity: Threats to Communications Networks and Public-Sector Responses"
March 28, 2012
(As Prepared for Delivery)

Heeding the call of the House Republican Cybersecurity Task Force, this subcommittee has embarked on a series of hearings to get a complete picture of the cybersecurity challenges our nation faces. Today is the third of our hearings on this topic, having already heard from witnesses in our previous hearings on the concerns of the private sector security firms helping to secure communications networks from cyberthreats as well as the network operators that must protect their networks while providing the broadband services that have become the fuel of our economy. Those hearings provided us with valuable information. This hearing continues our subcommittee's review of cybersecurity issues with a focus on the public sector.

In order to further investigate the complex issues that surround any discussion of cybersecurity, I recently asked a number of my subcommittee colleagues to serve on a bipartisan working group tasked with gathering additional information. My vice chairman, Mr. Terry, Ranking Member Eshoo, have graciously served as co-chairs of the working group for the last few weeks along with Mr. Latta, Mr. Kinzinger, Ms. Matsui, and Mr. Doyle. The members of the working group and their staffs have met with a number of industry stakeholders and throughout their discussions a consistent theme has emerged: the need for the government and the private sector to work together to address cybersecurity. The findings of the working group are consistent with the message we have heard in our hearings on this matter from the private sector perspective. Today, we hear from some of the agencies within our government that are working to meet these threats, both in terms of what is being done to promote cybersecurity as well as how we can better secure our nation's communications networks.

In this hearing, we are privileged to have five witnesses that represent parts of the government that work to address the complex cybersecurity issues our nation faces every day. The work being done by these government agencies to help address cybersecurity is just the tip of the iceberg of what we can achieve when our private sector innovation and public sector resources are put to a common task. That's why I am a co-sponsor of H.R. 3523, the Cyber Intelligence Sharing and Protection Act, a bipartisan bill introduced by my Communications and Technology colleague and Chairman of the House Permanent Select Committee on Intelligence, Mike Rogers. H.R. 3523 makes common sense changes to the way our government and the private sector share cyberintelligence without compromising either the commercial broadband providers or the integrity of the intelligence community.

Similarly, the good work being done by industry stakeholders at the FCC on the Communications Security, Reliability and Interoperability Council – or CSRIC – to bring voluntary best practices to bear on the security of commercial networks is another example of the type of public-private cooperation that achieves results without mandates. It looks very similar to the Australian model that received favorable reviews at one of our previous hearings. To remain nimble and effective, codes of conduct like these should remain voluntary and should involve all stakeholders in the Internet ecosystem, not just ISPs.

In addition to hearing from these agencies on the good work that they are doing, I also expect to hear how you think we can improve the cooperation between the federal government and private industry as they work to combat cyberthreats. Having heard from the private sector, today's public sector perspective will give the members of the subcommittee a more complete picture of the cybersecurity landscape.

I thank the panelists for their testimony today, and I look forward to a lively discussion of these issues.

###